INTERIM CHANGE 2004-1 TO AIR FORCE INSTRUCTION (AFI) 33-202, NETWORK AND COMPUTER SECURITY

17 JUNE 2004

★This Air Force instruction (AFI) implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and establishes Air Force COMPUSEC requirements for information protection compliance with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; Title 10 U.S. Code, Section 2224 (Defense Information Assurance Program), Department of Defense Directive (DoDD) 8500.1, *Information Assurance (IA)*, October 24, 2002; Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003; DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997; Department of Defense (DoD) 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000; and CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]*. The Uniform Code of Military Justice applies to personnel who violate the specific prohibitions and requirements of this instruction. This instruction gives the directive requirements for the COMPUSEC component of the Information Assurance (IA) discipline as outlined in AFPD 33-2. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems. The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). Use of extracts from this instruction is encouraged. Additional instructions and manuals are listed on the Air Force Publishing web site at Uniform Resource Locator (URL): http://www.e-publishing.af.mil under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication.** Provide an information copy to HQ AFCA/WFP. Send any supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Provide a copy of each final supplement to HQ AFCA/ITXD. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS, *Records Disposition Schedule (RDS)* located at https://webrims.amc.af.mil/rds/index.cfm. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. See Attachment 1 for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

★SUMMARY OF REVISIONS

This update incorporates interim change (IC) 2004-1. The revision brings the foreign national administrator policy and the certifier criteria in-line with DoD policy. The other changes are administrative in nature and do not reflect policy change.

★4.2.3. Ports, Protocols, and Services (PPS). The Air Force PPS matrix is an ongoing effort to provide policy for usage of known PPS on the Air Force enterprise. System developers and others responsible for bringing new information systems onto the Air Force enterprise shall ensure their systems conform to PPS outlined in the matrix. ***NOTE:*** The matrix does not list PPS usage for every Air Force information system, rather it provides overall policy for PPS use; should a conflict arise between the matrix and other operational guidance, or if a required PPS is not listed or is incorrect, contact HQ AFCA/WFPS. The matrix will be periodically updated as new information is presented. The PPS matrix is located at the Air Force IP web page (https://private.afca.af.mil/ip). ***NOTE:*** AFI 33-137, *Ports, Protocols, and Services (PPS) Management,* will contain Air Force PPS policy guidance when published.

★4.3.3.2.3. Additional security related information on PDAs is at the AFCA product evaluation web page (https://private.afca.af.mil/prodeval).

★4.7.1. All Air Force locations with an Air Force Service Delivery Point (SDP) shall bulk encrypt all AF.MIL to AF.MIL traffic before it traverses the NIPRNET. This configuration is known as the AF-VPN. AF-VPN traffic shall pass unencrypted through an Intrusion Detection System (IDS) to be examined before passing through the Base Information Protection (BIP) firewalls. All traffic shall pass through the AF-VPN from Air Force base to Air Force base. Submit requirements for other VPNs to HQ AFCA/ITL (Infostructure Architecture Council [IAC] Secretariat).

★5.2.2. Non-U.S. citizens may perform system or network administration, or other IT specialist duties, categorized as IT-I and IT-II (formerly known as AIS-I and AIS-II) positions. For those IT-I and IT-II positions that DoD policy identify as conditionally allowed, the information system DAA must ensure the following criteria from DoDI 8500.2, *Information Assurance (IA) Implementation,* is met before granting access:

★5.2.2.1. Personnel security investigative levels for non-U.S. citizens must be equivalent to the investigative levels of U.S. citizens performing similar duties.

★5.2.2.2. Non-U.S. citizens must be under the immediate supervision of a U.S. citizen.

★5.2.3. Foreign nationals access to SIPRNET. The SIPRNET is a US-Only SECRET network. Foreign nationals will not be granted access to US-Only classified networks and terminals (e.g., US-Only Enclaves on SIPRNET) (see CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]).*

★6.1.2.5. Further information on the Air Force C4ISP, CoN, and CtO processes can be found at the following web sites: https://private.afca.af.mil/c4isp or https://private.afca.af.mil/con. AFIs currently under development will contain additional information and guidance.

★6.2.2. Certifier. The Certifier is crucial to the success of the entire C&A effort. See paragraph 2.14. for the Certifier's roles and responsibilities. The Certifier should be a government employee, when

possible, and should be trained to fill the position. See NSTISSI 4015, *National Training Standard for System Certifiers*.

★6.7.2. Records: C&A records created by this publication should be maintained according to Air Force Web-RIMS RDS, Table 33-25, Rules 5.02 and 5.03. CoN and CtO are program records that should be maintained according to Air Force Web-RIMS RDS, Table 33-4, Rule 25 and Table 63-9, Rule 5.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 100-235, *Computer Security Act of 1987*

Public Law 104-13, *The Paperwork Reduction Act of 1995*

Title 5 U.S. Code, Section 552a (Privacy Act)

Title 10 U.S. Code, Section 2224 (Defense Information Assurance Program)

FIPS Pubs 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

OMB Circular A-130, *Management of Federal Information Resources*

OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*

NDP-1, *National Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations*

NSTISSI 4012, *National Training Standard for Designated Approving Authority (DAA)*

NSTISSI 4015, *National Training Standard for System Certifiers*

NCSC-TG-15, *A Guide to Understanding Trusted Facility Management*

NCSC-TG-026, *A Guide to Writing the Security Features User's Guide for Trusted Systems*

★CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*

DoDI 5000.2, *Operation of the Defense Acquisition System*, May 12, 2003 (formerly DoD 5000.2-R)

DoD 5200.2-R, *Personnel Security Program,* January 1987, through Change 3, February 23, 1996

DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997

DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995, through Change 2, May 1 2000

DoD 5220.22-M Supplement 1, February 1995

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organization*, June 16, 1992

DoDD 5230.20, *Visits, Assignments, and Exchanges of Foreign Nationals*, August 12, 1998

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 6, 1984 w/Change 1, August 18, 1995

DoD 5400.7-R/AF Sup 1, *Freedom of Information Act (FOIA) Program*, 24 June 2002

DoDD 8000.1, *Management of DoD Information Resources and Information Technology,* February 27, 2002, w/Change 1, March 20, 2002

DoDD 8500.1, *Information Assurance*, October 24, 2002

DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 14 August 2002

International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130)

Export Administration Regulations (EAR)

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 16-201, *Disclosure of Military Information to Foreign Governments and International Organizations* (to be published)

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104*, Base-Level Planning and Implementation*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115, Volume 1, *Network Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-118, *Radio Frequency (RF) Spectrum Management*

★AFI 33-137, (Draft) *Ports, Protocols, and Services (PPS) Management* (to be published)

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-203, *Emission Security*

AFI 33-204, *Information Assurance Awareness Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-206, *Air Force Specialized Information Assurance Publications*

AFI 33-207, *Computer Security Assistance Program*

AFI 33-213*, DoD Public Key Infrastructure Management and Use*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

★AFI 33-230, *Information Assurance Assessment and Assistance Program*

★AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFI 36-8002*, Telecommuting Guidelines For Air Force Reservists and Their Supervisors*

AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*

AFMAN 33-214, Volume 1, *(S) Emission Security Assessments* (U)

AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews*

AFMAN 33-223, *Identification and Authentication*

★AFMAN 37-123, *Management of Records*

★AFMAN 37-139 DELETED

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFPAM 63-1701, *Program Protection Planning*

AFSSI 5020, *Remanence Security* (will become AFMAN 33-224)

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

★WEB-RIMS, *Records Disposition Schedule (RDS)*

Abbreviations and Acronyms

ADP–Automated Data Processing

AFCA–Air Force Communications Agency

AFCERT–Air Force Computer Emergency Response Team

AF-CIO–Air Force Chief Information Officer

AFI–Air Force Instruction

AFIWC–Air Force Information Warfare Center

AFMAN–Air Force Manual

AFMC–Air Force Materiel Command

AFPD–Air Force Policy Directive

AFSPC–Air Force Space Command

AFSSI–Air Force Systems Security Instruction

AIA–Air Intelligence Agency

AIS–Automated Information System

AP–Access Points

ASD/C3I–Assistant Secretary of Defense for Command, Control, Communications and Intelligence

ASD/NII–Assistant Secretary of Defense for Networks and Information Integration (replaces the term ASD/C3I)

ASIM–Automated Security Incident Monitoring

BIP–Base Information Protection

C4I–Command, Control, Communications, Computers, and Intelligence

C4ISP–C4I Support Plan

C&A–Certification and Accreditation

CAC–Common Access Card

CC–Common Criteria

CCB–Configuration Control Board

CERT–Computer Emergency Response Team

CITS–Combat Information Transport System

CJCSI–Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC–Computer Security

COMSEC–Communications Security

CoN–Certificate of Networthiness

CSO–Communications and Information Systems Officer

CtO–Certificate to Operate

DAA–Designated Approving Authority

DAC–Discretionary Access Control

DISA–Defense Information Systems Agency

DISN–Defense Information Systems Network

DITSCAP–DoD Information Technology Security Certification and Accreditation Process

DoD–Department of Defense

DoDD–Department of Defense Directive

DRU–Direct Reporting Unit

DSAWG–DISN Security Accreditation Working Group

EAL–Evaluation Assurance Level

EAR–Export Administration Regulations

EMSEC–Emission Security

FDO–Foreign Disclosure Office

FIPS–Federal Information Processing Standards

FOA–Field Operating Agency

FOUO–For Official Use Only

FTP–File Transfer Protocol

GIAP–GIG Interconnection Approval Process

GIG–Global Information Grid

GSU–Geographically Separated Units

IA–Information Assurance

IATO–Interim Approval to Operate

IDS–Intrusion Detection Service

I&A–Identification and Authentication

IPO–Information Protection Operations

IR–Infrared

ISP–Internet Service Provider

ISSM–Information System Security Manager

ISSO–Information System Security Officer

IT–Information Technology

ITAR–International Traffic in Arms Regulations

i-TRM–Infostructure Technical Reference Model

JP–Joint Publication

MAC–Media Access Control

MAJCOM–Major Command

MFD–Multi-function Devices

NATO–North Atlantic Treaty Organization

NCC–Network Control Center

NCSC–National Computer Security Center

NIAP–National Information Assurance Partnership

NIPRNET–Non-Secure Internet Protocol Router Network

NIST–National Institute of Standards and Technology

NOSC–Network Operations and Security Center

NSA–National Security Agency

OMB–Office of Management and Budget

OPSEC–Operational Security

PC–Personal Computer

PDA–Personal Digital Assistants

PED–Personal Electronic Device

PKI–Public Key Infrastructure

P.L. –Public Law

POC–Point of Contact

PPS–Ports, Protocol, and Services

RAS–Remote Access Server

★RDS–Records Disposition Schedule

SABI–Secret and Below Interoperability

SAF–Secretary of the Air Force

SAF/AA–Administrative Assistant to the Secretary of the Air Force

SAP/SAR–Special Access Program/Special Access Required

SCAO–SIPRNET Connection Approval Office

SCD–Systems Compliance Database

SCI–Sensitive Compartmented Information

SDP–Service Delivery Point

SFUG–Security Feature User's Guide

SIPRNET–Secret Internet Protocol Router Network

SSAA–System Security Authorization Agreement

SSWG–System Security Working Group

ST&E–Security Test and Evaluation

TCNO–Time Compliance Network Order

TFM–Trusted Facility Manual

URL–Uniform Resource Locator

VPN–Virtual Private Network

WLAN–Wireless Local Area Network

WM–Workgroup Manager

Terms

Accountability--Process of tracing information systems activities to a responsible source.

Accreditation--Formal declaration by a DAA that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical managerial, and procedural safeguards.

Automated Information System (AIS)--An AIS is a collection of hardware and software sharing a common set of security policies, procedures, and mechanisms. AISs may consist of a single stand-alone computer, a central computer system with remote terminals (e.g., mainframe), a LAN, or a Wide Area Network (WAN).

Authentication--Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Category--A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification--Comprehensive evaluation of the technical and nontechnical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifier--Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Common Criteria--The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (IT) security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Computer-Based Security--Security for the information system is provided through the use of automated security features.

Computer Network--The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan or wide area and backbone networks.

Computing Environment--A computer workstation or server (host) and its operating system, peripherals, and applications.

Confidentiality--The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controlled Unclassified Information--Information that is not classified but has some restrictions placed on it, such as export controls or exemption from the Freedom of Information Act.

Controls--Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and nonconformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (***NOTE:*** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoDD 8000.1, *Management of DoD Information Resources and Information Technology,* February 27, 2002, w/Change 1, March 20, 2002, outlines internal controls for information systems.)

Countermeasures--Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system.

Designated Approving Authority (DAA)--Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Enclave--Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems.

They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Enclave Boundary--The point at which an enclave's internal network service layer connects to an external network's service layer.

Evaluation Assurance Level (EAL)--One of seven increasingly rigorous packages of assurance requirements from CC (Common Criteria (IS 15408)) Part 3. Each numbered package represents a point on the CC's predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

★**Foreign Nationals**--All individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees and contractors.

Formal Access Approval--Documented approval by a data owner to allow access to a particular category of information.

Functional System--A specific system used, owned, operated, and maintained by a functional community

Global Information Grid (GIG)--Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information

Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (f)). The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: 1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services. 2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services. 3. Processes data or information for use by other equipment, software, and services.

IA Product--Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or nonrepudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of nonauthorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

IA-Enabled Product--Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information 1.--Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (***NOTE:*** Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02).

Information Protection Operations (IPO)--A critical subcomponent of the Network Management function that implements and enforces national, DoD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from information system (IS) and network security intrusions. The NCC conducts IPO employing hardware and software tools to enhance the security of their networks

Information System--1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (***NOTE:*** This includes automated information

systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

Information Systems Security Manager (ISSM)--Principal advisor on computer security matters to DAA. (***NOTE:*** DoDI 8500.2 IA Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM)).

Information Systems Security Officer (ISSO)--Official who manages the COMPUSEC program for an information system assigned to him or her by the ISSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (***NOTE:*** DoDI 8500.2 IA Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

Integrity--Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Information Technology (IT)--Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

IT Position Category--Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in DoD 5200.2-R (reference (r)). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.

Level of Protection--Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Mission Assurance Category--Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to

determine the requirements for availability and integrity. DoD has three defined mission assurance categories:

Mission Assurance Category I--Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a category I system is unacceptable and could include the immediate and sustained loss of mission effectiveness. Category I systems require the most stringent protection measures.

Mission Assurance Category II--Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Category II systems require additional safeguards beyond best practices to ensure adequate assurance.

Mission Assurance Category III--Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Network Security Policy--Overall policy that is developed for the network. This policy regulates how sensitive and classified information is managed, protected, and distributed on the network. It also includes boundary protection, rules of engagement, methods of protection.

Nonrepudiation--Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing--Processing of various levels of classified and unclassified information at distinctly different times. (***NOTE:*** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.).

Privileged User--An authorized user who has access to system control, monitoring, or administration functions.

Program Manager--The person ultimately responsible for the overall procurement, development, integration, modification or operation and maintenance of the information system. (Synonymous with Single Manager or Project Manager.)

Safeguards--Protective measures and controls prescribed to meet the security requirements of an information system. (***NOTE:*** Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.).

Security Feature--A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; media access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information--Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (***NOTE:*** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Site Certification--Provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system is in accordance with the SSAA and a review of the local environment (threats/vulnerabilities).

Specified Robustness--The strength and level of confidence required of each IA solution is a function of the value of what is being protected (e.g., the mission assurance category or confidentiality level of the information being supported by the DoD information system) and the threat.

Stand-Alone System--An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System--Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

Strong Authentication--Two of the three approved methods of authentication: something you know (password), something you have (token), or something you are (biometric).

System Integrity--The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy--Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (***NOTE:*** It interprets regulatory [e.g., DoDD 8500.1, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.).

Tampering--Unauthorized modification that alters the proper functioning of information system security equipment.

Threat--Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User--Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability--1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM)--A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.